Theoretical Computer Science 443 (2012) 70–81

Contents lists available at SciVerse ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

Groups and decompositions of codes☆

Yun Liu*

Department of Mathematics, Yuxi Normal University, Yuxi, Yunnan, 653100, PR China

ARTICLE INFO

Article history:
Received 16 February 2012
Received in revised form 16 March 2012
Accepted 21 March 2012
Communicated by D. Perrin

Keywords:
Decomposition of codes
Group of codes
Maximal code
Rectangular group code
Variable-length code

ABSTRACT

In this paper, some relations between the decompositions of codes and the groups of codes are investigated. We first show the existence of an indecomposable, recognizable, and maximal code X such that the group $G(X)$ is imprimitive, which implies that the answer to a problem put forward by Berstel, Perrin, and Reutenauer in their book "Codes and Automata" is negative. Then, we discuss a special kind of code, that is, rectangular group codes, and show that a completely simple code is a rectangular group code if and only if it can be decomposed as a composition of a complete and synchronized code and a group code.

1. Introduction

Let A be a nonempty set called an *alphabet* whose elements are called *letters*. Finite sequences of elements of A are called *words* over A. Let A^* be the set of all words, which is a monoid under the concatenation operation of two words; the empty sequence is the identity element called the *empty word*, and is denoted by 1. The monoid A^* is called the *free monoid* on A. Let $A^+ = A^* \setminus \{1\}$. If $w = a_1a_2 \cdots a_n$ is a word with $a_i \in A$, then n is called the *length* of w, and is denoted by $|w|$. For $a \in A$, the number of occurrences of a in w is denoted by $|w|_a$. For any $w \in A^*$, denote by $\mathrm{alph}(w)$ the set of letters occurring in w. Let $\mathrm{alph}(X) = \bigcup_{w\in X} \mathrm{alph}(w)$ for any $X \subseteq A^*$.

$x \in A^*$ is called a *prefix* (respectively, *suffix*) of $y \in A^*$ if there exists a $u \in A^*$ such that $y = xu$ (respectively, $y = ux$). $x \in A^*$ is called a *factor* of $y \in A^*$ if there exist $u, v \in A^*$ such that $y = uxv$.

Usually, subsets of A^* are called *languages* over A. $X \subseteq A^*$ is called a *prefix set* (respectively, *suffix set*) if no element of X is a prefix (respectively, suffix) of another element of X. X is called a *bifix set* if it is both a prefix set and a suffix set. Let X be a language over A. The submonoid (respectively, subsemigroup) generated by X is denoted by X^* (respectively, X^+).

The following algebraic tool is useful in investigating languages. For any subset X of a monoid M, the relation

$$\sigma_X = \left\{(x, y) \in M \times M \mid (\forall u, v \in A^*)\ uxv \in X \text{ if and only if } uyv \in X\right\}$$

is a congruence on M, called the *syntactic congruence* of X. The quotient monoid $\mathbf{M}(X) = M/\sigma_X$ is called the *syntactic monoid* of X. The canonical homomorphism φ_X from M onto $\mathbf{M}(X)$ is called the *syntactic homomorphism* of X.

For an equivalence ρ of a monoid M, we often use $x\rho y$ to represent $(x, y) \in \rho$; that is, x and y are in the same ρ-class.

A nonempty subset I of a semigroup S is called an *ideal* of S if $IS \cup SI \subseteq I$. An ideal I of S is said to be *minimal* if there is no ideal of S properly contained in I. Since, for any two ideals I and J of a semigroup S, $IJ \subseteq I \cap J$, we know that, if a minimal

☆ The research is supported by the National Natural Science Foundation of China (Grant No. 11101354) and the Natural Science Foundation of Yunnan Province, China (Grant No. 2008ZC162M).

* Tel.: +8608772053601.
E-mail addresses: slliuyun@163.com, slliuyun@sina.com.

0304-3975/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2012.03.040

ideal of S exists, then it is unique. We call the unique minimal ideal K of S (if it exists) the *kernel* of S, and denote it by $\ker(S)$. Clearly $\ker(S)$ exists if and only if the intersection of all ideals of S is not empty. In this case, $\ker(S) = \bigcap \{I \mid I \text{ is an ideal of } S\}$. Notice that, if $\ker(S)$ exists, it is a simple semigroup (a semigroup is said to be simple if it has no proper ideal).

A subset X of a monoid M is said to be *dense* in M if it meets all ideals of M. Dense subsets of A^* are called *dense languages*. Clearly, a language $X \subseteq A^*$ is dense if any word $w \in A^*$ is a factor of some word in X. A language which is not dense is said to be *thin*. If X^* is dense in A^*, then X is said to be *complete*. A language X is said to be *very thin* if there exists a word $x \in X^*$ which is not a factor of word in X. Clearly, any very thin language is thin. Conversely, a thin language is not always very thin. However, a thin and complete language is very thin (see Section 9.4 of [1]).

Let $X \subseteq A^+$. X is called a *code* over A if any word $w \in A^*$ has at most one X-factorization. That is,

$$x_1x_2\cdots x_m = y_1y_2\cdots y_n, \quad x_i, y_j \in X, i = 1, 2, \ldots, m, j = 1, 2, \ldots, n$$

implies that $m = n$ and $x_i = y_i$, $i = 1, 2, \ldots, n$.

It is well known that a prefix set (respectively, suffix set, bifix set) other than $\{1\}$ is a code, which is called a *prefix code* (respectively, *suffix code*, *bifix code*).

We now introduce a proposition which characterizes the submonoid X^* of A^* for a code (respectively, prefix code, suffix code, bifix code) X. Let M be a monoid. A submonoid N of M is said to be *stable* in M if, for any $u, v, w \in M, u, v, uw, wv \in N$ implies that $w \in N$. N is said to be *right unitary* (respectively, *left unitary*) in M if, for any $u, v \in M, u, uv \in N$ implies that $v \in N$ (respectively, $u, vu \in N$ implies that $v \in N$). N is said to be *biunitary* in M if it is both right and left unitary.

Any submonoid M of A^* has a unique minimal set X of generators (see Proposition 2.2.1 of [1]). X is usually called the *base* of M.

Proposition 1.1 (*Propositions 2.2.3, 2.2.5, and 2.2.7 of [1]*). *A submonoid M of A^* is stable (respectively, right unitary, left unitary, biunitary) if and only if its base is a code (respectively, prefix code, suffix code, bifix code) over A.*

A [prefix, suffix, bifix] code X over A is said to be *maximal* if, for any $w \in A^* \setminus X, X \cup \{w\}$ is not a [prefix, suffix, bifix] code over A. On maximal codes, the following theorem is fundamental.

Theorem 1.2 (*Theorems 2.5.5 and 2.5.13 of [1]*). *Any maximal code is complete. Conversely, any thin and complete code is maximal.*

The class of group codes plays a critical role in the theory of codes. Let G be a group, let H be a subgroup of G, and let $\varphi : A^* \to G$ be a surjective homomorphism. Then the base X of the submonoid $\varphi^{-1}(H)$ is a code called a *group code* over A. It is well known that any group code is a bifix code as well as a maximal code. This class of codes has many remarkable properties; see Sections 2.2 and 11.3 of [1] for details.

We now give the concept of compositions of codes, which can be found in Section 2.6 of [1]. Let Y and Z be two codes over B and A, respectively, with $B = \text{alph}(Y)$. If there exists a bijection β from B onto Z, then the codes Y and Z are called composable (through β). Notice that such a bijection β can be extended to an injective homomorphism from B^* to A^* (see Proposition 2.1.1 of [1]), and hence $X = \beta(Y)$ is a code contained in Z^+ (see Corollary 2.1.6 of [1]), which is called the composition of Y and Z (by means of β), and is denoted by $X = Y \circ_\beta Z$, or simply $X = Y \circ Z$ when the context permits it.

Let G be a transitive permutation group over Q. An imprimitivity equivalence of G is an equivalence relation θ over Q that is stable for the action of G. The action of G on the classes of θ defines a transitive permutation group over Q/θ, denoted by G_θ, called the imprimitivity quotient of G for θ. For any $q \in Q$, denote by $[q]$ the equivalence class of q mod θ. Let K_q be the transitive permutation group over $[q]$ formed by the restrictions to $[q]$ of the permutations $g \in G$ that globally stabilize $[q]$. It can be easily checked that the groups K_q, $q \in Q$, are all equivalent. Any one of these groups is called the *induced group* of G on the classes of θ, and is denoted by G^θ. A transitive permutation group G over Q is said to be *primitive* if the only imprimitivity equivalences of G are the equality relation and the universal relation over Q. A transitive permutation group G over Q is said to be *regular* if all elements of G other than the identity have no fixed point. For more about permutation groups, see [8], for instance.

Let X be a very thin code over A, let $\mathcal{A}_D^*(X)$ be the flower automaton of X, and let φ_D be the associated representation. The *group of the code X* is, by definition, the Suschkewitch group of the monoid $\varphi_D(A^*)$, denoted by $G(X)$. It is a transitive permutation group of finite degree, and its degree is called the *degree of the code X*, denoted by $d(X)$ (see Section 9.5 of [1]). If the group $G(X)$ is a regular permutation group, we also say that the code X is *regular* (see Definition 4.7 of [6]). Some recent progress on groups of prefix codes can be found in the survey paper [2].

The following proposition tells us that we can construct codes with given groups from suitable syntactic monoids.

Proposition 1.3 (*See Exercises 9.5.1 of [1]*). *Let X be a thin and complete code, let $M = \mathbf{M}(X^*)$, let $K = \ker(M)$, let H be an $\mathscr{H}$-class in K that meets $\varphi(X^*)$, and let $H' = \varphi(X^*) \cap H$. Then the representation of H over the right cosets of H' is injective, and the permutation group obtained is equivalent to $G(X)$.*

The following proposition shows the basic relations about the groups of codes and the decompositions of codes.

Proposition 1.4 (*Proposition 11.1.2 of [1]*). *Let X be a very thin code which decomposes into $X = Y \circ Z$, with Y a complete code. Then there exists an imprimitivity equivalence θ of $G = G(X)$ such that*

$$G^\theta = G(Y), \qquad G_\theta = G(Z).$$

In particular, $d(X) = d(Y)d(Z)$.

The converse of the above proposition also holds in the case of maximal prefix codes.

Proposition 1.5 (*Proposition 11.1.6 of [1]*). *Let X be a thin and maximal prefix code. If the group $G = G(X)$ admits a imprimitivity equivalence θ, then there exists a decomposition of X into*

$$X = Y \circ Z$$

such that $G^\theta = G(Y)$ and $G_\theta = G(Z)$.

In [1], the authors put forward the following problem.

Problem 1.6 (*See Appendix of [1]*). *Does Proposition 1.5 hold for arbitrary thin and maximal codes?*

Proposition 1.5 has the following consequence.

Corollary 1.7 (*Corollary 11.1.7 of [1]*). *Let X be a thin and maximal prefix code. If X is indecomposable, then the group $G(X)$ is primitive.*

Then the following problem can be naturally raised.

Problem 1.8. *Let X be an indecomposable, thin and maximal code. Is the group $G(X)$ primitive?*

Clearly, if the answer to Problem 1.6 is positive, so is the answer to Problem 1.8.
The following proposition describes regular, thin, and maximal prefix codes.

Proposition 1.9 (*Proposition 11.2.3 of [1]*). *Let X be a thin and maximal prefix code. Then X is regular if and only if*

$$X = U \circ V \circ W,$$

where V is a regular group code and U, W are synchronized codes.

One can ask whether the above proposition holds for arbitrary thin and maximal codes. Clearly, by Proposition 1.4, the sufficiency has no problem. How about the necessity? We have the following.

Problem 1.10. *Let X be a regular, thin, and maximal code. Are there a regular group code V and two synchronized codes U, W such that*

$$X = U \circ V \circ W?$$

In the next section, we will construct an example to show that the answers to the above three problems are all negative. In Section 3, we investigate decompositions of rectangular group codes. A code X is a rectangular group code if $\ker(\mathbf{M}(X^*))$ is a rectangular group. This class of codes is defined in [6] and includes group codes and complete and synchronized codes as subclasses. We will show in Section 3 that a completely simple code is a rectangular group code if and only if it can be decomposed as a composition of a complete and synchronized code and a group code. In the last section, we give some concluding remarks and problems related to this works.

2. An indecomposable code with imprimitive groups

Let X be a language over A. A homomorphism φ from A^* onto a monoid M is said to *recognize* X if

$$\varphi^{-1}(\varphi(X)) = X.$$

In this case, we also say the monoid M *recognizes* X. X is said to be *recognizable*[1] if it is recognized by a finite monoid. It can be easily shown that the syntactic homomorphism φ_X recognizes X. Furthermore, we have the following.

Lemma 2.1 (*See Proposition 1.4.4 of [1]*). *Let $X \subseteq A^*$, and let $\varphi : A^* \to M$ be a surjective homomorphism recognizing X. Then there exists a homomorphism ψ from M onto $\mathbf{M}(X)$ such that $\varphi_X = \psi \circ \varphi$. Consequently, $\mathbf{M}(X)$ is the least monoid recognizing X in the sense that $\mathbf{M}(X)$ is a homomorphic image of every monoid M recognizing X.*

Thus we have the following well-known result.

Corollary 2.2. *A language X over A is recognizable if and only if $\mathbf{M}(X)$ is finite.*

$X \subseteq M$ is said to be *disjunctive* in a monoid M if $\sigma_X = 1_M$, the equality relation on M. The following lemma can be easily deduced from the definition of disjunctivity and Lemma 2.1.

Lemma 2.3 (*See [4]*). *If X is a language over A, then $\varphi_X(X)$ is a disjunctive subset of $\mathbf{M}(X)$.*
Conversely, if M is a monoid containing a disjunctive subset N, $\varphi : A^* \to M$ is a surjective homomorphism, and $X = \varphi^{-1}(N)$, then $M \cong \mathbf{M}(X)$.

Proof. See Proposition 5.3 in Chapter 6 of [4] and its proof for details. □

[1] Recognizable languages are also called regular languages in some literature, but we **do not** use this name, since the term "regular" has already represented another concept in this paper (see Section 1).

The following two lemmas are obvious.

Lemma 2.4. *Let $X \subseteq A^*$, and let φ be a homomorphism from A^* onto a monoid M recognizing X. Then X is a stable (respectively, right unitary, left unitary, biunitary) submonoid of A^* if and only if $\varphi(X)$ is a stable (respectively, right unitary, left unitary, biunitary) submonoid of M.*

Lemma 2.5. *Let $X \subseteq A^*$, and let φ be a homomorphism from A^* onto a monoid M recognizing X. Then X is dense in A^* if and only if $\varphi(X)$ is dense in M.*

The following proposition is a consequence of Proposition 1.1, Corollary 2.2, and Lemmas 2.3–2.5, which is useful in our main construction.

Proposition 2.6. *If X is a recognizable and complete code over A, then $\mathbf{M}(X^*)$ is finite and $\varphi_{X^*}(X^*)$ is a disjunctive, dense, and stable submonoid of $\mathbf{M}(X^*)$.*

Conversely, if M is a finite monoid containing a disjunctive, dense, and stable submonoid N, $\varphi : A^* \to M$ is a surjective homomorphism, and X is the base of $\varphi^{-1}(N)$, then X is a recognizable and complete code over A and $M \cong \mathbf{M}(X^*)$.

Before going on, to fix notation, we need give a brief introduction to the structure of completely simple semigroups.

A semigroup S is said to be *completely regular* or a *union of groups* if S is a disjoint union of a family of groups. A completely regular and simple semigroup is called a *completely simple semigroup*. Detailed information about completely regular semigroups and completely simple semigroups can be found in [3] and [7].

Let G be a group, let I and Λ be two nonempty sets, and let $P = (p_{\lambda i})$ be a $\Lambda \times I$-matrix with entries in G. Then $I \times G \times \Lambda$ is a semigroup under the following multiplication:

$$(i, g, \lambda)(j, h, \mu) = (i, gp_{\lambda j}h, \mu).$$

This semigroup is called a *Rees $I \times \Lambda$-matrix semigroup over the group G with sandwich matrix P and index sets I and Λ*, and is denoted by $\mathscr{M}(I, G, \Lambda; P)$. Any such kind of semigroup is briefly called a *Rees matrix semigroup*. The identity of the above group G is denoted by ι in this paper. The following Rees Theorem is well known.

Lemma 2.7 (*Rees Theorem; see Theorem III.2.6 of [7]*)**.** *A semigroup S is completely simple if and only if it is isomorphic to a Rees matrix semigroup $\mathscr{M}(I, G, \Lambda; P)$.*

The Rees matrix semigroup $\mathscr{M}(I, G, \Lambda; P)$ isomorphic to S in the above lemma is called a *Rees matrix representation* of S.

Let $S = \mathscr{M}(I, G, \Lambda; P)$, let $x = (i, g, \lambda)$, and let $y = (j, h, \mu) \in S$. Then it is clear that $x\mathscr{R}y$ if and only if $i = j$; $x\mathscr{L}y$ if and only if $\lambda = \mu$; and $x\mathscr{H}y$ if and only if $i = j$ and $\lambda = \mu$, where $\mathscr{R}$, $\mathscr{L}$ and $\mathscr{H}$ are Green relations. $x = (i, g, \lambda)$ is an idempotent if and only if $g = p_{\lambda i}^{-1}$, the group inverse of $p_{\lambda i}$ in G.

Now, we give the main construction of this section.

Definition 2.8. Let $I = \Lambda = \{1, 2, 3\}$, let $G = \mathbb{Z}/4\mathbb{Z}$ be the cyclic group of order 4, and let $P = (p_{\lambda i})$ be a $\Lambda \times I$-matrix over G defined as

$$P = \begin{pmatrix} \iota & \alpha & \iota \\ \alpha & \iota & \iota \\ \iota & \iota & \iota \end{pmatrix},$$

where ι is the identity of G and α is a generator of G. Let $K = \mathscr{M}(I, G, \Lambda; P)$ be the Rees $I \times \Lambda$-matrix semigroup over the group G with sandwich matrix P and index sets I and Λ. Let $s \notin K$, and let $M = K \cup \{1, s\}$. We define a multiplication "$\cdot$" on M as follows.

(1) 1 is the identity of the multiplication.

(2) For any $x, y \in K$, the multiplication of x and y follows the definition of the semigroup K.

(3) For $i = 1, 2, 3$, define

$$i^* = \begin{cases} i + 1 & \text{if } i = 1, 2; \\ 3 & \text{if } i = 3. \end{cases} \tag{2.1}$$

And, for any $x = (i, g, \lambda) \in K$, let

$$s \cdot x = (i^*, \alpha^2 g, \lambda) \tag{2.2}$$

and

$$x \cdot s = (i, g\alpha^2, \lambda^*). \tag{2.3}$$

(4) $s \cdot s = (3, \iota, 3)$.

Finally, let

$$N = \{(i, \iota, \lambda) \mid i, \lambda \in \{1, 3\}\} \cup \{1\}.$$

In the rest of this section, M and N follow the above definition.

Proposition 2.9. *M is a finite monoid and N is a disjunctive, dense, and stable submonoid of M.*

Proof. Clearly, M contains $3 \times 4 \times 3 + 2 = 38$ elements. Since M is finite, one can easily check the proposition by using a computer program. However, we still give a traditional mathematical proof below.

(1) We first show that M is a monoid. For this, we need only check the associative law:

$$(\forall x, y, z \in M)\ (x \cdot y) \cdot z = x \cdot (y \cdot z). \tag{2.4}$$

Clearly, by the definition of M, if $x, y, z \in K$ or at least one of x, y, z equals 1, then (2.4) holds. So we need only discuss the following cases.

(i) $x = s$ and $y, z \in K$. Suppose that $y = (i, g, \lambda)$ and $z = (j, h, \mu)$. Then

$$\begin{aligned}(x \cdot y) \cdot z &= (s \cdot (i, g, \lambda)) \cdot (j, h, \mu)\\ &= (i^*, \alpha^2 g, \lambda) \cdot (j, h, \mu)\\ &= (i^*, \alpha^2 g p_{\lambda j} h, \mu)\\ &= s \cdot (i, g p_{\lambda j} h, \mu)\\ &= s \cdot ((i, g, \lambda) \cdot (j, h, \mu))\\ &= x \cdot (y \cdot z).\end{aligned}$$

(ii) $x, y \in K$ and $z = s$. Similar to (i).

(iii) $x, z \in K$ and $y = s$. First, notice that, for any $i \in I$, $\lambda \in \Lambda$,

$$p_{\lambda^* i} = \alpha \Leftrightarrow i = 1, \lambda = 1 \Leftrightarrow p_{\lambda i^*} = \alpha.$$

This shows that $p_{\lambda^* i} = p_{\lambda i^*}$. Now, suppose that $x = (i, g, \lambda)$ and $z = (j, h, \mu)$. Then

$$\begin{aligned}(x \cdot y) \cdot z &= ((i, g, \lambda) \cdot s) \cdot (j, h, \mu)\\ &= (i, g\alpha^2, \lambda^*) \cdot (j, h, \mu)\\ &= (i, g\alpha^2 p_{\lambda^* j} h, \mu)\\ &= (i, g\alpha^2 p_{\lambda j^*} h, \mu)\\ &= (i, g p_{\lambda j^*} \alpha^2 h, \mu)\\ &= (i, g, \lambda) \cdot (j^*, \alpha^2 h, \mu)\\ &= (i, g, \lambda) \cdot (s \cdot (j, h, \mu))\\ &= x \cdot (y \cdot z).\end{aligned}$$

(iv) $x \in K$ and $y = z = s$. Suppose that $x = (i, g, \lambda)$. Then

$$\begin{aligned}(x \cdot y) \cdot z &= ((i, g, \lambda) \cdot s) \cdot s\\ &= (i, g\alpha^2, \lambda^*) \cdot s\\ &= (i, g\alpha^2\alpha^2, (\lambda^*)^*)\\ &= (i, g, 3) \quad (\text{since } (\lambda^*)^* \text{ always equals } 3.)\\ &= (i, g, \lambda) \cdot (3, \iota, 3)\\ &= (i, g, \lambda) \cdot s^2\\ &= x \cdot (y \cdot z).\end{aligned}$$

(v) $x = y = s$ and $z \in K$. Similar to (iv).

(vi) $x = z = s$ and $y \in K$. Suppose that $y = (i, g, \lambda)$. Then

$$\begin{aligned}(x \cdot y) \cdot z &= (s \cdot (i, g, \lambda)) \cdot s\\ &= (i^*, \alpha^2 g, \lambda) \cdot s\\ &= (i^*, \alpha^2 g\alpha^2, \lambda^*)\\ &= s \cdot (i, g\alpha^2, \lambda^*)\\ &= s \cdot ((i, g, \lambda) \cdot s)\\ &= x \cdot (y \cdot z).\end{aligned}$$

Therefore, M is a finite monoid.

(2) Clearly, $\{(i, \iota, \lambda) \mid i, \lambda \in \{1, 3\}\}$ is a subsemigroup of the completely simple semigroup K. Hence N is a submonoid of M.

(3) It can be easily checked that N is dense in M; that is,

$$(\forall w \in M)(\exists u, v \in M)\ uwv \in N.$$

In fact, if $w = (i, g, \lambda) \in K$, we need only let $u = (3, g^{-1}, 3)$ and $v = (3, \iota, 3)$; if $w = s$, we need only let $u = (3, \alpha^2, 3)$ and $v = (3, \iota, 3)$; if $w = 1$, we let $u = v = (3, \iota, 3)$. Then $uwv = (3, \iota, 3) \in N$.

(4) We now prove that N is stable in M; that is,

$$(\forall u, v, w \in M)\ u, uw, wv, v \in N \Rightarrow w \in N. \tag{2.5}$$

If at least one of u, v, w equals 1, then (2.5) holds trivially. So, we can suppose that $u, v, w \neq 1$. Then $u, v \in N$ implies that $u, v \in K$. Let $u = (i, \iota, \lambda)$ and let $v = (j, \iota, \mu)$.

If $w = s$, then, by (2.2) and (2.3), $uw = (i, \alpha^2, \lambda^*) \notin N$, $wv = (j^*, \alpha^2, \mu) \notin N$. So, we can suppose that $w \neq s$; that is, $w \in K$.

Now, suppose that $w = (k, g, \nu)$. Then $uw = (i, p_{\lambda k}g, \nu)$ and $wv = (k, gp_{\nu j}, \mu)$. So, $u, uw, wv, v \in N$ implies that $i, j, k, \lambda, \mu, \nu \in \{1, 3\}$ and $p_{\lambda k}g = gp_{\nu j} = \iota$. Then $p_{\lambda k} = p_{\nu j} = \iota$. So $g = \iota$. Therefore, $w \in N$. That is, (2.5) holds.

(5) Finally, we prove that N is disjunctive in M; that is, $\sigma_N = 1_M$. For this, we need only show that the following Property (D) holds for any x and y with $x \neq y$. □

Property (D) There exist $u, v \in M$ such that exactly one of the two elements uxv and uyv is in N.

It is useful to observe that, if exactly one of x and y is in N, then Property (D) holds with $u = v = 1$. So we can suppose that $x, y \in N$ or $x, y \notin N$. We consider the following cases.

(i) $x, y \notin K$; that is, $x, y \in \{1, s\}$. This case has just been excluded by the fact that $x, y \in N$ or $x, y \notin N$.

(ii) $x = (i, g, \lambda) \in K$ and $y = 1$ ($x = 1$ and $y \in K$ can be discussed symmetrically). Then $x \in N$. Let $u = (i, p_{2i}^{-1}, 2)$, and let $v = 1$. Then $uxv = x \in N$ and $uyv = u \notin N$.

(iii) $x = (i, g, \lambda) \in K$ and $y = s$ ($x = s$ and $y \in K$ can be discussed symmetrically).

If $\lambda \in \{1, 3\}$, letting $u = (1, g^{-1}p_{1i}^{-1}, 1)$ and $v = 1$, then $uxv = (1, \iota, \lambda) \in N$ and $uyv = (1, g^{-1}p_{1i}^{-1}\alpha^2, 2) \notin N$.

If $\lambda = 2$, letting $u = (3, \alpha^2, 3)$ and $v = 1$, then $uxv = (3, \alpha^2 g, 2) \notin N$ and $uyv = (3, \iota, 3) \in N$.

(iv) $x, y \in K$. Suppose that $x = (i, g, \lambda)$ and $y = (j, h, \mu)$.

If $i \neq j$, without loss of generality, we suppose that $i < j$. Then $(i, j) = (1, 2)$, $(2, 3)$, or $(1, 3)$.

If $i = 1$ and $j = 2$, letting $u = 1$ and $v = (3, g^{-1}, 1)$, then $uxv = (1, \iota, 1) \in N$ and $uyv = (2, hg^{-1}, 1) \notin N$.

$i = 2$ and $j = 3$ can be discussed similarly.

If $i = 1$ and $j = 3$, letting $u = s$ and $v = (3, h^{-1}\alpha^2, 3)$, then $uxv = (2, gh^{-1}, 3) \notin N$ and $uyv = (3, \iota, 3) \in N$.

Therefore, if $i \neq j$, then Property (D) holds. So we can suppose that $i = j$ in the following discussion. Symmetrically, we can suppose that $\lambda = \mu$. Since $x \neq y$, we have $g \neq h$; that is, $g^{-1}h \neq \iota$. Let $u = (3, g^{-1}, 3)$ and let $v = (3, \iota, 3)$. Then $uxv = (3, \iota, 3) \in N$ and $uyv = (3, g^{-1}h, 3) \notin N$.

Thus, in all cases, Property (D) holds, and hence N is disjunctive in M.

Clearly, by Definition 2.8, M is generated by the two elements $r = (1, \alpha, 1)$ and s. Now let $A = \{a, b\}$, and let $\varphi : A^* \to M$ be a homomorphism which maps a and b to r and s, respectively. Then φ is surjective. Let X be the base of $\varphi^{-1}(N)$. Then, by Propositions 2.6 and 2.9, X is a recognizable and complete (hence maximal) code over A and $M \cong \mathbf{M}(X^*)$. By the construction of M and Proposition 1.3, $G(X) \cong \mathbb{Z}/4\mathbb{Z}$ is a regular and imprimitive group.

Proposition 2.10. *The code X is indecomposable.*

Proof. Suppose that $X = Y \circ Z$ and $Z \neq X$. We need only prove that $Z = A$.

$X = Y \circ Z$ implies that $X^* \subseteq Z^*$. Let $N' = \varphi(Z^*)$. Then $N = \varphi(X^*) \subseteq N'$. Moreover, we have that the above inclusion is proper. In fact, if $N = N'$, then

$$Z^* \subseteq \varphi^{-1}(N') = \varphi^{-1}(N) = X^*.$$

Hence $Z^* = X^*$, and then $Z = X$, since X and Z are codes, a contradiction. That is, N' is a submonoid of M properly containing N. We complete the proof with the following two steps.

(1) We first show that $t = (3, \alpha^2, 3) \in N'$.

Let m be an element in $N' \setminus N$.

If $m = s$. Then $t = m^3 \in N'$. So we can suppose that $m \in K$.

Let $m = (i, \alpha^j, \lambda)$, where $i, \lambda \in \{1, 2, 3\}$ and $j \in \{0, 1, 2, 3\}$.

If $j \in \{1, 2, 3\}$, let $m' = (3, \iota, 3)$. Since $m' \in N \subseteq N'$, we have

$$(3, \alpha^j, 3) = m'mm' \in N'.$$

So, if $j = 2$, then $t \in N'$; if $j = 1, 3$, then $t = (3, \alpha^j, 3)^2 \in N'$.

If $j = 0$, since $m \notin N$, at least one of i and λ must be 2 in this case. Without loss of generality, we suppose that $i = 2$. Let $m'' = (3, \iota, 1)$. Since $m'' \in N \subseteq N'$, we have

$$t = (3, \alpha, 3)^2 = (m''mm')^2 \in N'.$$

(2) Now, by using (1), we show that $Z = A$.

First, since $t \in N' = \varphi(Z^*)$, there exists a word $z \in Z^*$ such that $\varphi(z) = t$. Since $ts = st = (3, \iota, 3) \in N$ and $\varphi(b) = s$, we have

$$zb, bz \in \varphi^{-1}((3, \iota, 3)) \subseteq \varphi^{-1}(N) = X^* \subseteq Z^*.$$

Hence $z, zb, bz \in Z^*$ implies that $b \in Z^*$ by the stability of Z^*. This implies that $s = \varphi(b) \in N \subseteq N'$.

Table 1
A nondeterministic automaton.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
a	2	3	4	1, 5	-	-	2	3	4	1, 5	-	3	1, 5	4
b	6	7	8	9	10	1, 11	12	6, 14	13	-	14	13	12	-

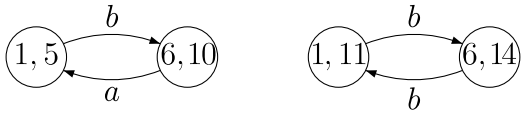

Fig. 1. The action on nontrivial subsets.

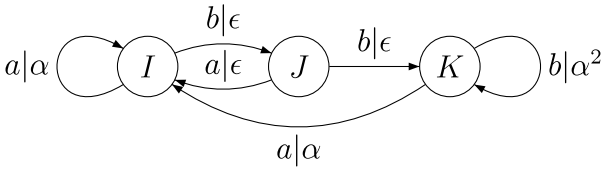

Fig. 2. The action on four-element subsets.

Second, since $p = (1, \iota, 1) \in N \subseteq N'$, we have

$$q = (1, \alpha^3, 1) = psp \in N' = \varphi(Z^*).$$

Then there exists a word $z' \in Z^*$ such that $\varphi(z') = q$. Since $qr = rq = p \in N$ and $\varphi(a) = r$, we have

$$z'a, az' \in \varphi^{-1}(p) \subseteq \varphi^{-1}(N) = X^* \subseteq Z^*.$$

Hence $z', z'a, az' \in Z^*$ implies that $a \in Z^*$ by the stability of Z^*.

Now $a, b \in Z^*$ clearly implies that $a, b \in Z$, since a and b are indecomposable. That is, $A \subseteq Z$, which implies that $Z = A$, since Z is a code.

Then we have the following theorem.

Theorem 2.11. *There exists an indecomposable, regular, recognizable, and maximal code X such that the group $G(X)$ is imprimitive. In particular, the answers to Problems 1.6, 1.8 and 1.10 are all negative.*

Dominique Perrin (personal communication) has given an unambiguous automaton recognizing the code X, as explained below. This presentation avoids having to verify the associative law of the monoid M.

Consider the nondeterministic automaton $\mathcal{A} = (Q, 1, 1)$ on the alphabet $A = \{a, b\}$ given by its transitions in Table 1.

The action of the letters a, b on pairs of states reachable from a single state is shown in Fig. 1. It shows that there is no letter which collapses any of these pairs, and thus that the automaton $\mathcal{A}$ in unambiguous.

Let $\varphi_{\mathcal{A}}(A^*)$ be the transition monoid of $\mathcal{A}$. The minimal rank of the elements of $\varphi_{\mathcal{A}}(A^*)$ is 4. Indeed $\varphi_{\mathcal{A}}(a)$ is of rank 4 with $I = \{\{1, 5\}, 2, 3, 4\}$ as the set of nonzero rows, and the action of the letters on I gives two other sets of four-element subsets:

$$J = \{\{6, 10\}, 7, 8, 9\}, \qquad K = \{\{1, 11\}, 12, \{6, 14\}, 13\}.$$

The action of the letters on these sets is indicated in Fig. 2. The second component of the label in Fig. 2 corresponds to the right Schützenberger representation of $\varphi_{\mathcal{A}}(A^*)$ relative to the idempotent $e = r^4$ and the coordinate system formed of the pairs (s, r), (s^2, r^4) with $r = \varphi_{\mathcal{A}}(a)$ and $s = \varphi_{\mathcal{A}}(b)$. The permutation α is the cycle (1234) on the set of fixpoints of e.

The minimal ideal of $\varphi_{\mathcal{A}}(A^*)$ is a 3×3 $\mathscr{D}$-class represented in Fig. 3. The sets U, V, W are the sets of nonzero columns of the elements r, sr, and s^2r, which are the following.

$$\begin{aligned} U &= \{\{1, 7\}, \{2, 8, 12\}, \{3, 9, 14\}, \{4, 10, 13\}\} \\ V &= \{\{2, 6\}, \{3, 7, 13\}, \{4, 8, 11\}, \{5, 9, 12\}\} \\ W &= \{\{1, 8\}, \{2, 9, 12\}, \{3, 6\}, \{4, 7, 13\}\}. \end{aligned}$$

Now, it is clear that $\varphi_{\mathcal{A}}(A^*)$ is isomorphic to the monoid M defined in Definition 2.8, and that X^* is recognized by the automaton $\mathcal{A}$.

	I	J	K
U	r	rs	rs^2
V	sr		
W	s^2r		s^2

Fig. 3. The minimal ideal of $\varphi_{\mathcal{A}}(A^*)$.

From Theorem 2.11, we know that the relationship between a code X and its group $G(X)$ is complicated in general. In the next section, we shall show that, if $\ker(\mathbf{M}(X^*))$ is orthodox (i.e., the multiplication of any two idempotents is also an idempotent), then the code X has a pretty good decomposition.

3. Decompositions of rectangular group codes

To characterize the compositions of maximal codes, the author defines a class of codes called completely simple codes in Section 3 of [5] and systematically characterizes this class of codes in [6].

A code X over A is said to be *completely simple* if $\ker(\mathbf{M}(X^*))$ is a complete simple semigroup. The well-known thin codes are particular kinds of completely simple codes (see Theorem 2.7 of [6]). Keeping the following hierarchy of codes in mind is helpful:

$$\mathbf{F} \subsetneq \mathbf{R} \subsetneq \mathbf{T} \subsetneq \mathbf{CS},$$

where **F**, **R**, **T**, and **CS** represent classes of finite codes, recognizable codes, thin codes, and completely simple codes, respectively.

Rectangular group codes are special kinds of completely simple codes which are defined and studied in Section 3 of [6]. This class of codes is a kind of generalization of group codes. In this section, we shall give a combinatorial characterization of rectangular group codes by using code decompositions.

A semigroup S is called a

- *right zero semigroup* if $xy = y$ for any $x, y \in S$;
- *left zero semigroup* if $xy = x$ for any $x, y \in S$;
- *rectangular band* if $x^2 = x$ and $xyx = x$ for any $x, y \in S$, or, equivalently, S is isomorphic to the direct product of a left zero semigroup and a right zero semigroup;
- *right group* if S is isomorphic to the direct product of a right zero semigroup and a group;
- *left group* if S is isomorphic to the direct product of a left zero semigroup and a group;
- *rectangular group* if S is isomorphic to the direct product of a rectangular band and a group.

The class of rectangular groups is an important subclass of completely simple semigroups. Right (respectively, left) zero semigroups, rectangular bands, groups, and right (respectively, left) groups are all subclasses of rectangular groups.

Rectangular groups have the following useful equivalent characterization.

Lemma 3.1 (*Theorem III.5.2 of [7]*)**.** *A completely simple semigroup S is a rectangular group if and only if S is orthodox (that is, the multiplication of any two idempotents of S is also an idempotent).*

Now, we begin to discuss some subclasses of completely simple codes, each of which can be defined by a certain subclass of completely simple semigroups.

From Theorem 2.5 of [6], we know that, if X is a complete code over A, then X is a group code if and only if $\ker(\mathbf{M}(X^*))$ is a group. This motivates us to give the following definition.

Definition 3.2 (*Definition 3.2 of [6]*)**.** Let $\mathscr{K}$ be a class of completely simple semigroups. A complete code X is called a *$\mathscr{K}$-code* if $\ker(\mathbf{M}(X^*)) \in \mathscr{K}$. In particular, X is called a *right group code* (respectively, *left group code*, *rectangular group code*) if $\ker(\mathbf{M}(X^*))$ is a right group (respectively, left group, rectangular group).

For the class of rectangular group codes and its subclasses, the author gives some characterizations in [6].

Lemma 3.3 (*Theorem 3.3 of [6]*)**.** *Let X be a complete code. Then X is a right group code (respectively, left group code, group code) if and only if X is a rectangular group code and a prefix code (respectively, suffix code, bifix code).*

Synchronized codes are important kinds of very thin codes when we study the groups of codes since we have the following.

Lemma 3.4 (*Proposition 10.1.11 of [1]*)**.** *A code is synchronized if and only if it has degree* 1.

Synchronized codes also have many practical applications owing to their good combinatorial properties. The definition and systematic characterizations of synchronized codes can be found in Section 3.6 and 10.1 of [1]. In particular, complete and synchronized codes have the following useful characterization.

Lemma 3.5 (*See Section 10.1 of [1]*). *Let $X \subseteq A^+$ be a code. Then X is complete and synchronized if and only if there exists a word $x \in X^*$ such that $xA^*x \subseteq X^*$.*

Complete and synchronized codes are also particular kinds of rectangular group codes, as shown in the following lemma.

Lemma 3.6 (*Corollary 3.5 of [6]*). *Let X be a complete code. Then X is a synchronized code (respectively, synchronized prefix code, synchronized suffix code) if and only if* $\ker(\mathbf{M}(X^*))$ *is a rectangular band (respectively, right zero semigroup, left zero semigroup).*

To prove our main result of this section, we need the following lemmas.

Lemma 3.7 (*Lemma 3.4 of [5]*). *Let X be a code over A, let $M = \mathbf{M}(X^*)$, let $\varphi = \varphi_{X^*}$, and let G be a subgroup of M. If $H = \varphi(X^*) \cap G$ is not empty, then it is a subgroup of G. In particular, if a subgroup G of M meets $\varphi(X^*)$, then the identity of the group G is contained in $\varphi(X^*)$.*

Lemma 3.8 (*Proposition 4.3 of [6]*). *Let X be a completely simple and complete code, let $M = \mathbf{M}(X^*)$, let $K = \ker(M)$, let H be an $\mathscr{H}$-class in K, let e be the identity of the group H, and let $H' = \varphi(X^*) \cap H$. Then $\{e\}$ is the only normal subgroup of H contained in H'.*

Lemma 3.9. *Let $X = Y \circ Z$ such that X is a completely simple and complete code and Z a bifix code. Then φ_{X^*} recognizes Z^*. Hence there exists a homomorphism ψ from $\mathbf{M}(X^*)$ onto $\mathbf{M}(Z^*)$ such that $\varphi_{Z^*} = \psi \circ \varphi_{X^*}$. In particular, $\mathbf{M}(Z^*)$ is a homomorphic image of $\mathbf{M}(X^*)$.*

Proof. By Lemma 2.1, we need only show that φ_{X^*} recognizes Z^*.

Let $M = \mathbf{M}(X^*)$, let $K = \ker(M)$, and let $\varphi = \varphi_{X^*}$. Since X is completely simple, K is a completely simple semigroup. Since X is complete, $\varphi(X^*) \cap K \neq \emptyset$. Let $e \in \varphi(X^*) \cap K$. Then, by Lemma 3.7, we can suppose that e is an idempotent. Let $x \in \varphi^{-1}(e)$. Then

$$x \in \varphi^{-1}(\varphi(X^*)) = X^* \subseteq Z^*.$$

To prove φ recognizes Z^*, we need to show that

$$(\forall m \in \varphi(Z^*))\ \varphi^{-1}(m) \subseteq Z^*.$$

Let H be the $\mathscr{H}$-class of e. We discuss this in the following three steps.

(1) We first consider a special case; that is, $m \in H$. Let m' be the group inverse of m, let $z \in \varphi^{-1}(m) \cap Z^*$, and let $y \in \varphi^{-1}(m')$. Then

$$zy, yz \in \varphi^{-1}(e) \subseteq \varphi^{-1}(\varphi(X^*)) = X^* \subseteq Z^*. \tag{3.1}$$

Hence $z, zy, yz \in Z^*$ implies that $y \in Z^*$ by the stability of Z^*. Notice that (3.1) also holds for any $z \in \varphi^{-1}(m)$. Hence $y, zy, yz \in Z^*$ implies that $z \in Z^*$ by the stability of Z^* again. Thus, $\varphi^{-1}(m) \subseteq Z^*$.

(2) We next consider a slightly general case; that is, $m\mathscr{R}e$. In this case, $me \in H$. Since $m, e \in \varphi(Z^*)$, $me \in \varphi(Z^*)$. Then, by (1), $\varphi^{-1}(me) \subseteq Z^*$. So, for any $y \in \varphi^{-1}(m)$, $yx \in \varphi^{-1}(me) \subseteq Z^*$, and $x \in Z^*$ implies that $y \in Z^*$, since Z is a suffix code. Thus, $\varphi^{-1}(m) \subseteq Z^*$.

(3) We now consider the general case. Clearly, $em\mathscr{R}e$, since K is the completely simple kernel of M. And $m, e \in \varphi(Z^*)$ implies that $em \in \varphi(Z^*)$. Then, by (2), $\varphi^{-1}(em) \subseteq Z^*$. So, for any $y \in \varphi^{-1}(m)$, $xy \in \varphi^{-1}(em) \subseteq Z^*$, and $x \in Z^*$ implies that $y \in Z^*$, since Z is a prefix code. Thus, $\varphi^{-1}(m) \subseteq Z^*$ for all $m \in \varphi(Z^*)$.

Now we are ready to obtain our main result of this section.

Theorem 3.10. *Let X be a completely simple code. Then X is a rectangular group code if and only if $X = Y \circ Z$ for some complete and synchronized code Y and group code Z.*

Proof. ($\Rightarrow$) Let X be a rectangular group code over A, let $M = \mathbf{M}(X^*)$, let $K = \ker(M)$, and let $\varphi = \varphi_{X^*}$. Then K is a rectangular group. Let e be an idempotent of K such that the $\mathscr{H}$-class H of e meets $\varphi(X^*)$ and $H' = \varphi(X^*) \cap H$. Then, by Lemma 3.7, H' is a subgroup of the group H and, in particular, $e \in \varphi(X^*)$.

Now, we consider a mapping $\psi : A^* \to H$ which maps each $w \in A^*$ to $e\varphi(w)e$. Clearly, ψ is surjective. We show that it is a homomorphism as follows. Since K is a rectangular group, $K \cong I \times G \times \Lambda$ for some left zero semigroup I, group G, and right zero semigroup Λ. Let $e = (i, \iota, \lambda)$, where ι is the identity of G. For any $x, y \in A^*$, since $e\varphi(x)\mathscr{R}e$ and $\varphi(y)e\mathscr{L}e$, we have $e\varphi(x) = (i, g, \mu)$ and $\varphi(y)e = (j, h, \lambda)$ for some $j \in I, g, h \in G$, and $\mu \in \Lambda$. Then $e\varphi(x)e = (i, g, \mu)(i, \iota, \lambda) = (i, g, \lambda)$, $e\varphi(y)e = (i, \iota, \lambda)(j, h, \lambda) = (i, h, \lambda)$, and

$$\begin{aligned}
\psi(xy) &= e\varphi(xy)e \\
&= e\varphi(x)\varphi(y)e \\
&= (i, g, \mu)(j, h, \lambda) \\
&= (i, gh, \lambda) \\
&= (i, g, \lambda)(i, h, \lambda) \\
&= (e\varphi(x)e)(e\varphi(y)e) \\
&= \psi(x)\psi(y).
\end{aligned}$$

Let Z be the base of $\psi^{-1}(H')$. Then Z is a group code. Since $\psi(X^*) = e\varphi(X^*)e = H'$, we have $X^* \subseteq Z^*$. Notice that X is a maximal code,[2] we have $X = Y \circ_\beta Z$ by Proposition 2.6.14 of [1], where $\beta : B^* \to A^*$ is an injective homomorphism which maps B onto Z, and Y is a code over B.

We show that Y is complete and synchronized. Let $x \in \varphi^{-1}(e)$. Then $x \in X^*$. Moreover,

$$xZ^*x \subseteq \varphi^{-1}(\varphi(xZ^*x)) = \varphi^{-1}(e\varphi(Z^*)e) = \varphi^{-1}(\psi(Z^*)) = \varphi^{-1}(H') \subseteq \varphi^{-1}(\varphi(X^*)) = X^*.$$

Let $y \in \beta^{-1}(x)$. Then $x \in X^*$ implies that $y \in Y^*$ and $xZ^*x \subseteq X^*$ implies that $yB^*y \subseteq Y^*$. Then, by Lemma 3.5, Y is complete and synchronized.

($\Leftarrow$) Let $X = Y \circ_\beta Z$ with Y a complete and synchronized code over B and Z a group code over A, let $M = \mathbf{M}(X^*)$, let $K = \ker(M)$, let $N = \mathbf{M}(Z^*)$, let $\varphi = \varphi_{X^*}$, and let $\varphi' = \varphi_{Z^*}$. Then N is a group. We need to prove that K is a rectangular group.

By Lemma 3.9, φ recognizes Z^*, and there exists a homomorphism ψ from M onto N such that $\varphi' = \psi \circ \varphi$. We first show that the restriction of ψ to any $\mathscr{H}$-class in K is injective.

Since Y is a complete and synchronized code over A, $yB^*y \subseteq Y^*$ for some $y \in Y^*$. Let $x = \beta(y)$. Then $x \in X^* \subseteq Z^*$ and $xZ^*x \subseteq X^*$. Since, for any $w \in B^*$, $y' = ywy$ also satisfies the property $y'B^*y' \subseteq Y^*$, we can further suppose that $e = \varphi(x)$ is an idempotent in K. Let H be the $\mathscr{H}$-class of e and let $H' = \varphi(X^*) \cap H$.

We now prove that $\varphi(Z^*) \cap H = \varphi(X^*) \cap H$. Notice that, since $H = eMe = \varphi(xA^*x)$, we have, for any $m \in \varphi(Z^*) \cap H$, that there exists a word $w \in A^*$ such that $m = \varphi(xwx)$. Since $m \in \varphi(Z^*)$ and φ recognizes Z^*, we have $xwx \in Z^*$. Notice that, since Z is a bifix code and $x \in Z^*$, we have $w \in Z^*$. So $xwx \in xZ^*x \subseteq X^*$, and hence $m \in \varphi(X^*) \cap H$. Thus $\varphi(Z^*) \cap H \subseteq \varphi(X^*) \cap H$. Note that the inverse inclusion is clear, since $X^* \subseteq Z^*$. So we have $\varphi(Z^*) \cap H = \varphi(X^*) \cap H$.

Now, we are ready to prove a special case; that is, that the restriction of ψ to H is injective. We also denote by 1 the identity of N. Since $1 \in \varphi'(Z^*)$, φ' recognizes Z^*, and φ is surjective, we have

$$\psi^{-1}(1) \subseteq \psi^{-1}(\varphi'(Z^*)) = \varphi(\varphi^{-1}(\psi^{-1}(\varphi'(Z^*)))) = \varphi(\varphi'^{-1}(\varphi'(Z^*))) = \varphi(Z^*).$$

Hence

$$\psi^{-1}(1) \cap H \subseteq \varphi(Z^*) \cap H = \varphi(X^*) \cap H = H'.$$

Then $\psi\big|_H$, the restriction of ψ to H, is a group homomorphism from H to N with $\ker(\psi\big|_H) = \psi^{-1}(1) \cap H \subseteq H'$. This implies $\ker(\psi\big|_H) = \{e\}$, since $\{e\}$ is the only normal subgroup of H contained in H' by Lemma 3.8. Thus, the restriction of ψ to H is injective.

Next we cope with the general case. Let H_1 be an arbitrary chosen $\mathscr{H}$-class in K. Since K is a regular $\mathscr{D}$-class, there exist $s, s' \in M$ such that $\tau : m \mapsto s'ms$ is an isomorphism from H_1 onto H (see the proof of Proposition 2.3.6 of [3] for detail). We shall show that the restriction of ψ to H_1 is injective. In fact, if $m_1, m_2 \in H_1$ satisfy $\psi(m_1) = \psi(m_2)$, then

$$\psi(\tau(m_1)) = \psi(s'm_1s) = \psi(s'm_2s) = \psi(\tau(m_2)).$$

Since the restriction of ψ to H is injective, the above equation implies that $\tau(m_1) = \tau(m_2)$. Then $m_1 = m_2$, since τ is an isomorphism. Thus, the restriction of φ to H_1 is injective. Then, we have proved that the restriction of ψ to any $\mathscr{H}$-class in K is injective.

Now, we can easily deduce that K is a rectangular group. In fact, for any idempotents $e_1, e_2 \in K$, suppose that H_1 is the $\mathscr{H}$-class of e_1e_2 and that e_3 is the idempotent of H_1. Then we have $\psi(e_1) = \psi(e_2) = \psi(e_3) = 1$, since 1 is the only idempotent of N. So $\psi(e_1e_2) = 1$. Since the restriction of ψ to H_1 is injective and $e_1e_2, e_3 \in H_1$, we have $e_1e_2 = e_3$. Therefore, the multiplication of any two idempotents of K is also an idempotent. Then, by Lemma 3.1, K is a rectangular group, and hence X is a rectangular group code.

By Lemma 3.3 and Theorem 3.10, we have the following.

Corollary 3.11. *Let X be a completely simple code. Then X is a right (respectively, left) group code if and only if $X = Y \circ Z$ for some complete and synchronized prefix (respectively, suffix) code Y and group code Z.*

Note that the hypothesis "X is a completely simple code" in the above theorem and corollary is necessary. In fact, a composition of a complete and synchronized code Y and a group code Z is not necessary a completely simple code, as shown in the following example.

Example 3.12. Let $A = \{a, b\}$, let $Z = D$ be the Dyck code[3] over A, and let B be a countable infinite alphabet. Let

$$Z_1 = \left\{w \in Z \mid |w| = 2^n \text{ for some positive integer } n\right\}$$

and let $Z_2 = Z \setminus Z_1$. It can be easily checked that Z_1 and Z_2 are both countable infinite. Partition B into two countable infinite subsets B_1 and B_2, let $Y = B_2^*B_1$, and let β be an arbitrarily chosen bijection from B onto Z which maps B_i onto Z_i, $i = 1, 2$.

[2] A rectangular group code is always maximal since it is complete by its definition and the fact that any completely simple and complete code is maximal (see Theorem 2.8 of [6]).

[3] Dyck code is the base of the submonoid $\{w \in A^* \mid |w|_a = |w|_b\}$ of A^*.

Then, clearly, Y is a complete and synchronized prefix code over B, and Y and Z are composable through β. Let $X = Y \circ_\beta Z$. We show that X is not completely simple, as follows.

We first note that, since $B_1 \subseteq Y \subseteq Y^*$ and $B_2 \cap Y^* = \emptyset$, we have $Z_1 \subseteq X^*$ and $Z_2 \cap X^* = \emptyset$.

Next, we show that, if $(x, y) \in \sigma_{X^*}$, then $|x| = |y|$. Suppose on the contrary that $|x| \neq |y|$. Without loss of generality, suppose that $|x| > |y|$. Let $u, v \in A^*$ be such that $uxv \in Z^*$, let $p = |uxv|$, let $q = |uyv|$, let r be an integer such that $2^r \geq 3p$, let $u' = a^{p+(2^r-3p)/2}$, and let $v' = b^{p+(2^r-3p)/2}$. Then, clearly, $u'uxvv' \in Z$ and

$$\left|u'uxvv'\right| = \left|u'\right| + |uxv| + \left|v'\right| = (p + (2^r - 3p)/2) + p + (p + (2^r - 3p)/2) = 2^r.$$

Hence $u'uxvv' \in Z_1 \subseteq X^*$. Now, if $\left|u'uyvv'\right|_a \neq \left|u'uyvv'\right|_b$, then $u'uyvv' \notin Z^*$, and hence $u'uyvv' \notin X^*$. If $\left|u'uyvv'\right|_a = \left|u'uyvv'\right|_b$, then, by the choice of u' and v', $u'uyvv' \in Z$. Moreover, we have

$$\left|u'uyvv'\right| = \left|u'\right| + |uyv| + \left|v'\right| = (p + (2^r - 3p)/2) + q + (p + (2^r - 3p)/2) = 2^r - (p - q).$$

Since $2^r \geq 3p$, we have $2^{r-1} > p - q > 0$, and hence $2^{r-1} < \left|u'uyvv'\right| < 2^r$. Thus $u'uyvv' \in Z_2$, which implies that $u'uyvv' \notin X^*$, since $Z_2 \cap X^* = \emptyset$. Therefore, in any case, $u'uxvv' \in X^*$ and $u'uyvv' \notin X^*$. That is, $(x, y) \notin \sigma_{X^*}$, a contradiction.

Therefore, $(w, w^2) \notin \sigma_{X^*}$ for any $w \in A^+$ and $\{1\}$ is a singleton σ_{X^*}-class. Hence $\mathbf{M}(X^*) \setminus \{1\}$ is a subsemigroup that contains no idempotent. Then $\ker(\mathbf{M}(X^*))$ cannot be a completely simple semigroup, since completely simple semigroups contain idempotents. Thus X is not a completely simple code.

Since compositions of thin codes are always thin (see Proposition 2.6.4 of [1]) and a group code is thin if and only if it is recognizable (see Proposition 2.5.20 and Example 2.5.22 of [1]), Theorem 3.10 has the following corollary, which well characterizes thin rectangular group codes.

Corollary 3.13. *A code X is a thin rectangular group code (respectively, right group code, left group code) if and only if $X = Y \circ Z$ for some complete and synchronized code (respectively, prefix code, suffix code) Y and recognizable group code Z.*

Note that one can directly prove the above corollary, and the proof can be simplified by using Proposition 1.4 and Lemma 3.4.

Since a group code X over A is finite if and only if $X = A^d$ for some positive integer d (see Theorem 11.3.1 of [1]), we have the following.

Corollary 3.14. *A code X is a finite rectangular group code (respectively, right group code, left group code) if and only if $X = Y \circ A^d$ for some finite, complete and synchronized code (respectively, prefix code, suffix code) Y and positive integer d.*

In this case, d is the degree of X and the group $G(X)$ is cyclic. In particular, X is regular.

Note that, in general, a rectangular group code is not necessarily regular. In fact, the class of rectangular group codes and the class of regular completely simple codes are not comparable under set inclusion, as shown in Theorem 5.1 of [6]. On the other hand, a regular finite maximal code is not necessarily a rectangular group code (see the proof of Theorem 5.1 of [6]).

4. Conclusion remarks

We conclude this paper with some remarks.

First, we can now completely discuss the relationship between the indecomposability of codes and the primitivity of their groups. There are three cases.

(1) If X is a thin and maximal bifix code, then

$$X \text{ is indecomposable } \Leftrightarrow G(X) \text{ is primitive.}$$

(2) If X is a thin and maximal prefix code, then

$$X \text{ is indecomposable } \begin{array}{c}\Rightarrow \\ \not\Leftarrow\end{array} G(X) \text{ is primitive.}$$

(3) If X is a thin and maximal code, then

$$X \text{ is indecomposable } \begin{array}{c}\not\Rightarrow \\ \not\Leftarrow\end{array} G(X) \text{ is primitive.}$$

In fact, (1) is Theorem 11.4.7 of [1]. The arguments from left to right in (2) and (3) have been stated in Corollary 1.7 and Theorem 2.11, respectively. For the other direction, we need only let $X = Y \circ Z$ such that Y is a nontrivial synchronized maximal prefix code and Z is a nontrivial thin and maximal prefix code with $G(Z)$ primitive. Then, by Proposition 1.4 and Lemma 3.4, $G(X)$ is equivalent to $G(Z)$. Therefore, X is a decomposable, thin, and maximal prefix code with $G(X)$ primitive.

Second, the code X constructed in Section 2 is infinite. In fact, one can easily check that $a^2(ab)^n a^2 \in X$ for all nonnegative integers n. It is not known whether the counterexamples to Problems 1.6, 1.8 and 1.10 can be chosen to be finite. We cannot efficiently construct such examples by using this method, since, for a code X, we do not know any conditions for $\mathbf{M}(X^*)$ and $\varphi_{X^*}(X^*)$ to characterize the finiteness of X. Perhaps such a condition cannot easily be found since we do not even know any conditions for $G(X)$ to ensure a code X to be finite in general.

Third, it is natural to ask the following question: What is the relation between the decomposition of a thin and maximal code X and the structure of $\ker(\mathbf{M}(X^*))$ in general?

Finally, we know from this paper that, when we investigate the syntactic structure (including $\mathbf{M}(X^*)$ and $G(X)$) of a thin and maximal code X, the really complicated case is that the completely simple semigroup $\ker(\mathbf{M}(X^*))$ is not orthodox. So, we can exclude rectangular group codes when we study the syntactic structures of thin and maximal codes in many situations.

Acknowledgments

The author thanks Professor Dominique Perrin for his valuable comments and suggestions, which led to a substantial improvement of this paper.

References

[1] J. Berstel, D. Perrin, C. Reutenauer, Codes and Automata, Cambridge University Press, 2010.
[2] J. Berstel, C. De Felice, D. Perrin, C. Reutenauer, G. Rindone, Recent results on syntactic groups of prefix codes, European Journal of Combinatorics (2012), http://dx.doi.org/10.1016/j.ejc.2012.03.004.
[3] J.M. Howie, Fundamentals of Semigroup Theory, Oxford University Press, New York, 1995.
[4] G. Lallement, Semigroups and Combinatorial Applications, Wiley Interscience, New York, 1979.
[5] Y. Liu, Compositions of maximal codes, Theoretical Computer Science 411 (2010) 228–238.
[6] Y. Liu, Completely simple codes, Semigroup Forum (2011), http://dx.doi.org/10.1007/s00233-011-9351-5.
[7] M. Petrich, N.R. Reilly, Completely Regular Semigroups, A Wiley-Interscience Publication, 1999.
[8] H. Wielandt, Finite Permutation Groups, Academic Press, 1964.